KOBIL Chipkartenterminal KAAN Advanced (USB/RS232)

Security Target

Stand 30.05.2006

Version 1.19

KOBIL Systems GmbH
Pfortenring 11
67547 Worms

KOBIL secure your identity

Inhalt

ST-Einführung „ASE_INT.1“ 3
1.1. ST-Identifikation 3
1.2. ST-Übersicht 3
1.3. Postulat der Übereinstimmung mit den CC 4
2. EVG-Beschreibung „ASE_DES.1“ 5
3. EVG-Sicherheitsumgebung „ASE_ENV.1“ 9
3.1. Annahmen 9
3.2. Bedrohungen 10
4. Sicherheitsziele „ASE_OBJ.1“ 11
4.1. Sicherheitsziele für den TOE (EVG) 11
4.2. Sicherheitsziele für die Umgebung 11
5. IT-Sicherheitsanforderungen „ASE_REQ.1“ 13
5.1. Funktionale Sicherheitsanforderungen an den TOE (EVG) 13
5.2. Anforderungen an die Vertrauenswürdigkeit des TOE (EVG) 19
5.3. Sicherheitsanforderungen an die IT-Umgebung 20
6. EVG-Übersichtsspezifikation „ASE_TSS.1“ 21
6.1. EVG-Sicherheitsfunktionen 21
6.2. Maßnahmen zur Vertrauenswürdigkeit 23
7. PP-Postulate „ASE_PPC.1“ 24
8. Erklärung 24
8.1. Erklärung der Sicherheitsziele 24
8.2. Erklärung der Sicherheitsanforderungen 26
8.3. Erklärung der EVG-Übersichtsspezifikation 34
8.4. Erklärung der PP-Postulate 37
9. Literaturverzeichnis 38
10. Abkürzungsverzeichnis 40

1. ST-Einführung „ASE_INT.1“

Der Evaluations-Gegenstand sind die KOBIL Chipkartenterminals KAAN Advanced USB und KAAN Advanced RS232 in der folgenden Version:

Hardware - Version: **K104R3** (identisch bei USB- und RS232-Version)
Firmware - Version: **1.02**

Die Hardware-Version ist von aussen auf dem EVG für den Benutzer ersichtlich angegeben.

Die Chipkartenterminals sind in zwei Bauformen verfügbar: mit serieller (RS232) Schnittstelle und mit USB-Schnittstelle. In beiden Bauformen ist die gleiche zu evaluierende Firmware enthalten. Desweiteren wird auch die Modellreihe KAAN Base (USB/RS232) angeboten, die keine Tastatur zur gesicherten PIN-Eingabe enthält und NICHT Bestandteil dieser Evaluierung ist.

1.1. ST-Identifikation

Titel der Sicherheitsvorgaben:	KOBIL Chipkartenterminal KAAN Advanced (USB/RS232) Security Target
Version:	1.19
Ausgabedatum:	30.05.2006
Autor:	Markus Tak, KOBIL Systems GmbH
Bestätigungskennung:	BSI.02050.TE
Zertifizierungskennung:	BSI-DSZ-CC-0301

Es liegen die Common Criteria in Version 2.1 zugrunde.

1.2. ST-Übersicht

Die Chipkartenleser KOBIL KAAN Advanced USB und RS232 sind universelle Chipkartenlesegeräte mit Tastatur zur sicheren PIN-Eingabe sowie einer updatefähigen Firmware. Die robuste Ausführung sorgt für einen sicheren Stand auf dem Tisch und ermöglicht auch die einhändige Bedienung. Es werden alle gängigen asynchronen Prozessor-Chipkarten nach ISO/IEC 7816 [4] und EMV 2000 [10] sowie diverse Protokolle für synchrone Speicherchipkarten unterstützt. Die sichere PIN-Eingabe wird jedoch nur für asynchrone Prozessor-Chipkarten angeboten.

Das universelle Chipkartenterminal unterstützt eine große Anzahl von Betriebssystemen, die Microsoft Windows Treiber sind WHQL-zertifiziert und entsprechen internationalen Standards. Neben der qualifizierten Signatur werden viele weitere Chipkarten-basierte Anwendungen unterstützt, wie HBCI Homebanking, Datei- und Festplattenverschlüsselung, Windows Logon, VPN Authentisierung, Netzwerk-Zugang und Terminal Server Applikationen.

Im Unterschied zur evaluierten Modellreihe KAAN Advanced verfügt die zur gleichen Produktlinie gehörende Modellreihe KAAN Base USB/RS232 nicht über eine eigene Tastatur zur sicheren PIN-Eingabe.

Die RS232 Version ist Stecker-kompatibel zum B1 Standard [20] der Deutschen Telekom AG, die USB-Version unterstützt den Hersteller-übergreifenden CCID Standard [8].

Das Chipkartenterminal KAAN Advanced stellt einen Teil der Signatur-Anwendungs-komponente gemäß §2 SigG[6] dar:

- „Im Sinne dieses Gesetzes sind [...] 11. ‚Signaturanwendungskomponenten' Software- und Hardwareprodukte, die dazu bestimmt sind, a) Daten dem Prozess der Erzeugung oder Prüfung qualifizierter elektronischer Signaturen zuzuführen oder b) [...]"

und entspricht den Anforderungen des §15 SigV [7]:

- Abs. 2: „Signaturanwendungskomponenten nach § 17 Abs. 2 des Signaturgesetzes müssen gewährleisten, dass 1. bei der Erzeugung einer qualifizierten elektronischen Signatur a) die Identifikationsdaten nicht preisgegeben und diese nur auf der jeweiligen sicheren Signaturerstellungseinheit gespeichert werden [...]"

- Abs. 4: „Sicherheitstechnische Veränderungen an technischen Komponenten nach den Absätzen 1 bis 3 müssen für den Nutzer erkennbar werden."

1.3. Postulat der Übereinstimmung mit den CC

Die Sicherheitsvorgaben sind in ihren funktionalen Anforderungen konform zu den Vorgaben nach Teil 2 und in ihren Anforderungen zur Vertrauenswürdigkeit konform zu Teil 3 der Common Criteria (Version 2.1 August 1999) EAL3 mit Zusatz (ADO_DEL.2, ADV_IMP.1, ADV_LLD.1, ALC_TAT.1, AVA_MSU.3, AVA_VLA.4). Die Sicherheitsfunktionsstärke ist mit „SOF-hoch" eingestuft.

2. EVG-Beschreibung „ASE_DES.1“

Die KOBIL Chipkartenterminals KAAN Advanced USB und KAAN Advanced RS232 (im folgenden EVG genannt) stellen universelle Chipkartenlesegeräte dar, die Prozessorchipkarten nach ISO/IEC 7816 [4] und EMV 2000 [10] über verschiedene Applikationsschnittstellen (CT-API [1], PC/SC [3], OCF[13]) verarbeiten können.

Die Geräte arbeiten mit allen Chipkarten-Datenübertragungsprotokollen gemäß ISO/IEC 7816 [4] (T=0, T=1). Datenübertragungsprotokolle für Speicherchipkarten (I2C-, 2-Wire-, 3-Wire-Protokoll) werden ebenfalls unterstützt. Sie verfügen über ein Keypad mit Silikontasten, um eine sichere PIN-Eingabe zu garantieren. Es besitzt die numerischen Tasten „0“ bis „9“ sowie die Tasten „Korrektur“ (gelb), „Bestätigung“ (grün) und „Abbruch“ (rot), eine Stern-Taste („*“), eine Funktionstaste („F“) und eine Punkt-Taste („.“).

Der Leser erkennt die von der Host-Software übermittelten Kommandos zur PIN-Eingabe nach CT-BCS [2] bzw. CCID [8] und fügt die vom Benutzer über das Keypad eingegebenen Nummern als PIN an die entsprechenden Stellen des Kommandos an die Chipkarte ein. Dabei wird nur die Tatsache an den Host gemeldet, dass eine der numerischen Tasten gedrückt wurde. Dies dient der Host-Applikation dem Anwender zu visualisieren, dass er eine Taste gedrückt hat bzw. wie viele Ziffern der PIN aktuell eingegeben sind.

Die PIN selbst verlässt den Leser nie in Richtung Host. Die Leser können an allen Hostsystemen verwendet werden, die eine serielle RS232 bzw. eine USB Schnittstelle besitzen. Sie werden als Zubehör im PC-Umfeld eingesetzt. Die Stromversorgung erfolgt in der seriellen Konfiguration über die PS/2 Schnittstelle (Maus, Tastatur) und als USB-Gerät über den USB-Bus. Auf der Hostseite werden die Applikationsschnittstellen CT-API und PC/SC sowie OCF[13] zur Verfügung gestellt, die für alle Chipkartenarten genutzt werden können. Alle Funktionalitäten an den Schnittstellen werden für CT-API gemäß [1], für PC/SC gemäß [3] und für OCF gemäß [13] abgebildet.

Das ebenfalls in CT-BCS [2] enthaltene Kommando INPUT zur Tastatur-Eingabe wird auch unterstützt. Dabei kann der Benutzer Daten über die Tastatur des EVG eingeben, die dann zum Host geschickt werden. Um diesen Vorgang von der sicheren PIN-Eingabe zu unterscheiden, wird der Modus der sicheren PIN-Eingabe eindeutig durch eine LED angezeigt.

Die Treiber der Chipkartenleser sind nicht Bestandteil des EVG und unterstützen diverse Betriebssysteme. Die verfügbaren Treiber werden mit dem Produkt ausgeliefert.

Der EVG besitzt keine Funktionalität, die ohne Anschluss an einen Host arbeitet. Er muss generell an einem Host betrieben werden. Die Treibersoftware gehört nicht zum Evaluationsumfang. Der EVG endet an der seriellen RS232- bzw. USB-Schnittstelle zum Host-Rechner. Der EVG ist wegen seiner Multifunktionalität in vielen Marktsegmenten einsetzbar. Da die Chipkartenleser als Klasse 2 Leser [5] auch in der Lage sind, Identifikationsdaten (PIN) zu erfassen und an sichere Signaturerstellungseinheiten (Signatur-Chipkarten) nach §2 Nummer 10 SigG auf sicherem Weg zu übermitteln, können sie auch für Applikationen gemäß Signaturgesetz und Signaturverordnung ([6], [7]) eingesetzt werden. Sie dienen des Weiteren zur Übermittlung des Hash-Wertes von der Anwendung zur Signaturkarte und zur Rückübertragung der Signatur von der Karte zur Signaturanwendung. Sie stellen somit eine Teilkomponente für Signaturanwendungskomponenten dar, die eine

Sicherheitsbestätigung benötigen, um für qualifizierte elektronische Signaturen nach §2 Nummer 3 SigG eingesetzt werden zu können. Zur Verwendung des EVG gemäß SigG/SigV sind sowohl Applikationen (Signaturanwendungen) als auch Chipkarten, die im SigG-Kontext evaluiert und bestätigt wurden, einzusetzen.

Synchrone Speicherchipkarten, die naturgemäß nicht im Rahmen des Signaturgesetzes zur Signaturerstellung eingesetzt werden können, werden zwar auf Kommunikationsebene vom EVG unterstützt, die sichere PIN Eingabe ist für diesen Typ von Chipkarten jedoch nicht vorgesehen. Somit sind diese Chipkarten nicht für die Evaluierung relevant.

Der EVG erfüllt die speziellen Anforderungen nach §15 Absatz 2 Nr.1a (keine Preisgabe oder Speicherung der Identifikationsdaten ausserhalb der Sicheren Signatur Erstellungseinheit) und Absatz 4 (Erkennbarkeit sicherheitstechnischer Veränderungen) SigV. Nachfolgende Liste der zur sicheren PIN-Eingabe unterstützten Instruction-Bytes sind von den Applikationen zu verwenden und von den Chipkarten spezifikationsgemäß zu unterstützen bzw. bei Nicht-Unterstützung mit einer geeigneten Fehlermeldung abzulehnen:

- VERIFY (ISO/IEC 7816-4): INS=0x20
- CHANGE REFERENCE DATA (ISO/IEC 7816-8): INS=0x24
- ENABLE VERIFICATION REQUIR EMENT (ISO/IEC 7816-8): INS=0x28
- DISABLE VERIFICATION REQUIREMENT (ISO/IEC 7816-8): INS=0x26
- RESET RETRY COUNTER (ISO/IEC 7816-8): INS=0x2C
- UNBLOCK APPLICATION (EMV2000): INS=0x18

Die Auslieferung der KOBIL Chipkartenterminals KAAN Advanced USB und KAAN Advanced RS232 geschieht auf zwei Wegen: im „Urzustand“ mit einer darin enthaltenen Firmware, die bei der Produktion eingebracht wird, und die Möglichkeit zum Update der Firmware durch einen gesicherten „Download“, um für zukünftige Anforderungen vorbereitet zu sein.

Zum Lieferumfang der Produkte KOBIL Chipkartenterminals KAAN Advanced USB und KAAN Advanced RS232 gehören im Auslieferungsweg „Urzustand“ neben dem Chipkartenterminal mit vorinstallierter Firmware (Teil des EVG) noch eine gedruckte Benutzeranleitung (Teil des EVG) und eine CD-ROM mit Treibern und Software zum Auslesen der Firmware-Version (kein Teil des EVG).
In Auslieferungsweg „Download“ besteht der Lieferumfang aus der Firmware (Teil des EVG), einem Software-Tool zum Laden der Firmware in den EVG (kein Teil des EVG) und einer elektronischen Ergänzung zur Benutzerdokumentation mit Hinweisen für die korrekte Installation der Firmware (Teil des EVG). Die auf der CD-ROM enthaltenen Treiber und Software (kein Teil des EVG) ist ebenfalls über den Auslieferungsweg „Download“ zu beziehen.

Die Verifikation einer Signatur der Firmware mit dem asymmetrischen Elliptischen Kurven-Algorithmus (ECDSA) und einer Schlüssel-Länge von 192 Bit garantiert die Integrität und Authentizität der Firmware beim Laden der Firmware in den Chipkartenleser. Die Signatur-Prüfung wird dabei innerhalb des EVG von dessen Firmware durchgeführt. Nur nach erfolgreicher Signatur-Prüfung wird die neue Firmware aktiviert, andernfalls wird sie abgewiesen. Der Hersteller KOBIL Systems stellt ein Software-Tool bereit, das die Übertragung der Firmware an den EVG vornimmt und nicht Teil des EVG ist.

Die sichere Generierung und Verwaltung der für die Erzeugung der sicheren Signatur notwendigen Schlüssel werden durch den Hersteller KOBIL Systems gewährleistet. Der Hersteller garantiert, dass jede neue Version des EVGs eine neue Versionsnummer erhält und damit eindeutig identifizierbar ist. Wird eine neue, unbestätigte Firmware eingespielt, so verliert die Bestätigung ihre Gültigkeit. Eine neue Firmware muss einem neuen Bestätigungsverfahren unterzogen werden.

Die aktuell bestätigten Versionen der Firmware und der Hardware des EVG sind auf den Webseiten der Bundesnetzagentur (BNetzA) unter http://www.bundesnetzagentur.de für den Benutzer abrufbar, die zertifizierten Versionen beim Bundesamt für Sicherheit in der Informationstechnik (BSI) unter http://www.bsi.bund.de . Es obliegt der Verantwortung des Benutzers, sich hier vor der Installation einer neuen Firmware davon zu überzeugen, ob eine neu zu installierende Firmware Version nach SigG / SigV [6], [7] bestätigt und nach Common Criteria [11] zertifiziert ist. Die entsprechenden Downloads stellt der Hersteller KOBIL Systems auf seinen Webseiten unter http://www.kobil.de bzw. http://www.kobil.com bereit. Den Benutzern wird empfohlen, diese Webseiten regelmäßig zu besuchen, um sich über Aktualisierungen zu informieren.

Über eine standardisierte Schnittstelle nach CT-BCS [2] kann softwaremäßig vom Host aus die aktuell im EVG befindliche Firmware Version ausgelesen werden, die Hardware Version ist auf dem Typschild des EVG aufgebracht.

Das Gehäuse ist mittels einer fälschungssicheren, durch das BSI zertifizierten Versiegelung verschlossen, welche sich bei Entfernung zerstört und damit nur einmal verwendbar ist.

Der EVG ist ausschliesslich für den Einsatz im nicht-öffentlichen oder privaten Bereich konzipiert. Daher wird auf eine verschlüsselte Übertragung der Identifikationsdaten zwischen Chipkartenterminal und Chipkarte verzichtet.

In Abschnitt 6 sind die einzelnen Sicherheitsfunktionen spezifiziert, welche die folgenden Anforderungen aus §15 SigV [7], Abs. 2 und 4 wie folgt abdecken:

- Die Anforderungen aus §15 SigV [7], Abs. 2:
  „Signaturanwendungskomponenten nach § 17 Abs. 2 des Signaturgesetzes müssen gewährleisten, dass 1. bei der Erzeugung einer qualifizierten elektronischen Signatur a) die Identifikationsdaten nicht preisgegeben und diese nur auf der jeweiligen sicheren Signaturerstellungseinheit gespeichert[1] werden [...]“
  werden durch die folgenden Sicherheitsfunktionen abgedeckt:
  SF.CLMEM
  SF.PINCMD

- Die Anforderung aus §15 SigV [7], Abs. 4:
  „Sicherheitstechnische Veränderungen an technischen Komponenten nach den Absätzen 1 bis 3 müssen für den Nutzer erkennbar werden.“
  werden durch die folgenden Sicherheitsfunktionen abgedeckt:
  SF.SEAL
  SF.SECDOWN

Die Chipkartenleser demonstrieren verschiedene Betriebszustände mittels dreier LEDs und eines Summers wie folgt:

	LED1 (grün)	**LED2 (orange)**	**LED3 (gelb)**	**Summer**
EVG stromversorgt, Smartcard inaktiv	AN	AUS	AUS	AUS
EVG stromversorgt, Smartcard aktiviert	AN	AUS	AN	AUS
Sichere PIN-Eingabe	AN	Blinken	AN	Aufforderung: 3x piepsen (abschaltbar) Tasten-Echo: 1x piepsen (abschaltbar) Erfolg: 1x tieferer Piepton (abschaltbar) Misserfolg: 4x piepsen (abschaltbar)
Firmware-Update läuft	AUS	AUS	AN	AUS
Gerätefehler	Blinken	AUS	AN / AUS	AUS

[1] In diesem Dokument ist mit „Speicherung der Identitifikationsdaten“ die **dauerhafte** Speicherung der Identifikationsdaten gemeint, die über den zur Verarbeitung unbedingt notwendigen Umfang hinausgeht. Der „zur Verarbeitung unbedingt notwendige Umfang“ ist der Zeitraum zwischen Eingabe der PIN über die Tastatur und dem Senden des PIN-Kommandos an die Chipkarte.

3. EVG-Sicherheitsumgebung „ASE_ENV.1“

Dieses Kapitel beschreibt die Sicherheitsaspekte der Umgebung, in der der EVG eingesetzt wird, die zu schützenden Werte und die handelnden Subjekte (wie Benutzer und Angreifer). Des Weiteren sind die organisatorischen Sicherheitsmaßnahmen und Hinweise zur sicheren Nutzung des EVGs dargestellt. Die zu schützenden Werte sind die Identifikationsdaten (PIN) des Nutzers sowie die Firmware und Hardware des Chipkartenlesers selbst.

3.1. Annahmen

A.USER.RESP1:

Die Regeln zur sicheren Handhabung und Nichtweitergabe der PIN werden dem Anwender vom Herausgeber der Chipkarte mitgeteilt, insbesondere die unbeobachtete Eingabe der PIN.

A.USER.RESP2:

Während der PIN-Eingabe über das Keypad des Lesers überprüft der Endanwender den Status der LEDs dahingehend, dass der Mode der sicheren PIN-Eingabe aktiv ist.

A.USER.RESP3:

Zertifizierte bzw. bestätigte Firmware, die von KOBIL Systems zum Download angeboten wird, ist durch Angabe der Zertifizierungs- bzw. Bestätigungs-IDs gekennzeichnet. Der Endanwender überzeugt sich vor der Installation einer neuen Firmware davon, dass diese nach SigG/SigV [6], [7] bestätigt und nach Common Criteria[11] zertifiziert ist.

A.USER.RESP4:

Der Endanwender prüft die Versiegelung vor jeder PIN-Eingabe auf Unversehrtheit.

A.USER.RESP5:

Der EVG wird ausschliesslich im nicht-öffentlichen oder privaten Bereich eingesetzt.

A.USER.RESP6:

Für die qualifizierte Signatur wird der EVG nur in Verbindung mit Signatur-Chipkarten (Sichere Signatur-Erstellungseinheit, SSEE) verwendet, die den Anforderungen des SigG/SigV [6], [7] entsprechen.

A.USER.RESP7:

Für die qualifizierte Signatur wird der EVG nur in Verbindung mit Signatur-Anwendungskomponenten verwendet, die den Anforderungen des SigG/SigV [6], [7] entsprechen.

3.2. Bedrohungen

Preisgabe der Identifikationsdaten
Die PIN als Identifikationsdaten des Anwenders stellt ein persönliches Geheimnis dar. Ihre Preisgabe ist eine direkte Bedrohung der Vertraulichkeit

T.REVEAL.1:
Der Angreifer könnte über ein trojanisches Pferd (Virus) versuchen, die Kommunikation zwischen Host und Chipkarte bzw. Chipkartenleser abzuhören, wenn die PIN in das Host-Gerät gelangt (passiver Angriff).

T.REVEAL.2:
Der Angreifer könnte versuchen, die PIN vom Benutzer unter Verwendung eines vorhandenen Befehls an den EVG zur Tastaturabfrage oder durch missbräuchliche Verwendung der sicheren PIN-Eingabe zu erlangen (aktiver Angriff).

Speicherung der Identifikationsdaten
Die dauerhafte Speicherung der PIN als Identifikationsdaten außerhalb der sicheren Signaturerstellungseinheit ist eine indirekte Bedrohung der Vertraulichkeit. Eine kurzzeitige Speicherung der Identifikationsdaten nur für den zur Verarbeitung unbedingt notwendigen Zeitraum ist jedoch nicht zu vermeiden.

T.STORE.1:
Durch die dauerhafte Speicherung der Identifikationsdaten im EVG besteht die Gefahr eines Angriffs darin, dass diese Daten durch einen Angreifer aus dem EVG ausgelesen werden könnten, wenn er in den Besitz des EVGs gelangt und technische Voraussetzungen hierfür besitzen würde.

Sicherheitstechnische Veränderungen
Modifizierungen sicherheitstechnischer Art geben einem Angreifer die Gelegenheit, die Identifikationsdaten im EVG abzugreifen und somit in Besitz der PIN zu gelangen.

T.MODIFY.1:
Durch eine modifizierte Firmware im EVG könnten die Sicherheitsfunktionen ausser Kraft gesetzt werden.

T.MODIFY.2:
Durch Manipulationen der Hardware nach Öffnen des Lesers kann der Angreifer die Kommunikation zwischen Leser und Chipkarte belauschen und damit die Identifikationsdaten (PIN) erfahren. Dies erreicht er durch einen Austausch von Hardware-Komponenten.

4. Sicherheitsziele „ASE_OBJ.1“

4.1. Sicherheitsziele für den TOE (EVG)

O.REVEAL:

Der EVG liest die Identifikationsdaten von der Tastatur ein und gibt sie – eingebettet in ein vom PC übertragenes Kommando-Template - ausschliesslich an die Signatur-Chipkarte weiter, sofern das Kommando-Template eines der zulässigen Kommandos (siehe Abschnitt 0) enthält.

O.MODE:

Der Modus der sicheren PIN Eingabe wird dem Endbenutzer durch den Status der LEDs eindeutig angezeigt.

O.STORE:

Der EVG speichert keine Identifikationsdaten ausserhalb des für die Verarbeitung unbedingt notwendigen Zeitraums.

O.MODIFY_DLD:

Die Modifikation der Firmware des EVG kann nur über eine gesicherte Software-Update Prozedur durchgeführt werden

O.MODIFY_SEAL:

Durch die Versiegelung sind Versuche, den EVG zu öffnen, für den Endanwender sichtbar.

4.2. Sicherheitsziele für die Umgebung

OE.USER.RESP1:

Die Regeln zur sicheren Handhabung und Nichtweitergabe der PIN müssen dem Endanwender vom Herausgeber der Chipkarte mitgeteilt werden, insbesondere die unbeobachtete Eingabe der PIN.

OE.USER.RESP2:

Während der PIN-Eingabe über das Keypad des Lesers muss der Endanwender den Status der LEDs dahingehend überprüfen, dass der Mode der sicheren PIN-Eingabe aktiv ist.

OE.USER.RESP3:

Zertifizierte bzw. bestätigte Firmware, die von KOBIL Systems zum Download angeboten wird, muss durch Angabe der Zertifizierungs- bzw. Bestätigungs-IDs gekennzeichnet sein. Der Endanwender muss sich vor der Installation einer neuen Firmware davon überzeugen, dass diese nach SigG/SigV [6], [7] bestätigt und nach Common Criteria[11] zertifiziert ist.

OE.USER.RESP4:

Der Endanwender muss die Versiegelung vor jeder PIN-Eingabe auf Unversehrtheit hin überprüfen.

OE.USER.RESP5:
Der EVG darf ausschliesslich im nicht-öffentlichen oder privaten Bereich eingesetzt werden.

OE.USER.RESP6:
Für die qualifizierte Signatur ist der EVG nur in Verbindung mit Signatur-Chipkarten (Sichere Signatur-Erstellungseinheit, SSEE) zu verwenden, die den Anforderungen des SigG/SigV [6], [7] entsprechen.

OE.USER.RESP7:
Für die qualifizierte Signatur ist der EVG nur in Verbindung mit Signatur-Anwendungskomponenten zu verwenden, die den Anforderungen des SigG/SigV [6], [7] entsprechen.

5. IT-Sicherheitsanforderungen „ASE_REQ.1“

5.1. Funktionale Sicherheitsanforderungen an den TOE (EVG)

Die Mindeststärkestufe der Funktionen ist „SOF-hoch“. Die Bewertung der algorithmischen Stärke der kryptographischen Operationen ist nicht Gegenstand der Evaluierung.

FCS_COP.1_ECDSA: Kryptographischer Betrieb
Ist hierarchisch zu: Keinen anderen Komponenten.

FCS_COP.1_ECDSA.1: Kryptographischer Betrieb
Die TSF müssen **die Entschlüsselung (asymmetrisch mit dem öffentlichen Schlüssel) als Bestandteil der Verifikation der Firmware-Signatur** *gemäß eines spezifizierten kryptographischen Algorithmus* **nach ECDSA (basierend auf dem Diskreten-Logarithmus-Problem in der Gruppe E(Fp)) gemäß SigG-Alg[12]** *und kryptographischer Schlüssellängen* **von 192 bit (Parameter p und q),** *die den folgenden* **Normen FIPS 186-2 [17], ISO/IEC 15946-2[18], ANSI X9.62[14] und IEEE 1363[15]** *entsprechen, durchführen.*

Abhängigkeiten:
[FDP_ITC.1 Import von Benutzerdaten ohne Sicherheitsattribute
oder
FDP_ITC.2 Import von Benutzerdaten mit Sicherheitsattributen
oder
FCS_CKM.1 Kryptographische Schlüsselgenerierung]
FCS_CKM.4 Zerstörung des kryptographischen Schlüssels
FMT_MSA.2 Sichere Sicherheitsattribute

FCS_COP.1_SHA: Kryptographischer Betrieb
Ist hierarchisch zu: Keinen anderen Komponenten.

FCS_COP.1_SHA.1: Kryptographischer Betrieb
Die TSF müssen **die Hash-Berechnung als Bestandteil der Verifikation der Firmware-Signatur** *gemäß eines spezifizierten kryptographischen Algorithmus* **nach SHA-1 gemäß SigG-Alg[12]** *und kryptographischer Schlüssellängen***, welche hierbei nicht relevant sind,** *die den folgenden* **Normen FIPS 180-2[16] und ISO/IEC 10118-3 [19]** *entsprechen, durchführen.*

Abhängigkeiten:
[FDP_ITC.1 Import von Benutzerdaten ohne Sicherheitsattribute
oder
FDP_ITC.2 Import von Benutzerdaten mit Sicherheitsattributen
oder
FCS_CKM.1 Kryptographische Schlüsselgenerierung]
FCS_CKM.4 Zerstörung des kryptographischen Schlüssels
FMT_MSA.2 Sichere Sicherheitsattribute

FDP_ACC.1: Teilweise Zugriffskontrolle
Ist hierarchisch zu: Keinen anderen Komponenten.

FDP_ACC.1.1:
Die TSF müssen die **Chipkartenleser-Zugriffspolitik** *für*
die Subjekte
S.USER: Benutzer über die Tastatur-Schnittstelle
S.PC: Host-PC über die RS232 bzw. USB-Schnittstelle
die Objekte
OB.PIN: PIN
und die durch die SFP abgedeckten Operationen
OP.P_ENTRY: sichere PIN-Eingabe
OP.P_CMD: PIN-Kommando vom Host
durchsetzen.

Abhängigkeiten:
FDP_ACF.1 Zugriffskontrolle basierend auf Sicherheitsattributen

Verfeinerung:
Zusammenhänge: Subjekte - Objekte - Operationen

	S.PC	S.USER
OB.PIN	OP.P_CMD	OP.P_ENTRY

FDP_ACF.1: Zugriffskontrolle basierend auf Sicherheitsattributen
Ist hierarchisch zu: Keinen anderen Komponenten.

FDP_ACF.1.1:
Die TSF müssen die **Chipkartenleser-Zugriffspolitik** *für Objekte, die auf* **keinen Sicherheitsattributen** *basieren, durchsetzen.*

FDP_ACF.1.2:
Die TSF müssen die folgenden Regeln durchsetzen, um festzustellen, ob eine Operation zwischen kontrollierten Subjekten und kontrollierten Objekten zulässig ist:

1. **Der Host-PC (S.PC) sendet Kommandos an den Leser, die den EVG nur dann dazu veranlasst, vom Benutzer (S.USER) eine PIN (OB.PIN) entgegenzunehmen und an die Chipkarte weiterzuleiten, wenn**
   a. **die Kommandos OP.P_CMD an den Chipkartenleser anhand ihrer Kommandostruktur gemäß CCID [8] bzw. CT-BCS [2] als solche zum Verifizieren bzw. Modifizieren der PIN erkennbar sind und außerdem**
   b. **ein an die Chipkarte weiterzuleitendes Kommando in OP.P_CMD mit einem der folgenden Instruction-Bytes enthalten ist:**
      i. **VERIFY (ISO/IEC 7816-4): INS=0x20**
      ii. **CHANGE REFERENCE DATA (ISO/IEC 7816-8): INS=0x24**
      iii. **ENABLE VERIFICATION REQUIREMENT (ISO/IEC 7816-8): INS=0x28**
      iv. **DISABLE VERIFICATION REQUIREMENT (ISO/IEC 7816-8): INS=0x26**
      v. **RESET RETRY COUNTER (ISO/IEC 7816-8): INS=0x2C**
      vi. **UNBLOCK APPLICATION (EMV2000): INS=0x18**
2. **Der Benutzer (S.USER) kann entscheiden, ob die von ihm eingegebene (OP.P_ENTRY) PIN (OB.PIN) vom EVG an die Chipkarte gesendet wird (grüne Bestätigungstaste) oder nicht (rote Abbruchtaste).**

FDP_ACF.1.3:
Die TSF müssen den Zugriff von Subjekten auf Objekte basierend auf den folgenden zusätzlichen Regeln explizit autorisieren: **keine.**

FDP_ACF.1.4:
Die TSF müssen den Zugriff von Subjekten auf Objekte, basierend auf **keinen weiteren Regeln**, *explizit verweigern.*

Abhängigkeiten:
FDP_ACC.1 Teilweise Zugriffskontrolle
FMT_MSA.3 Initialisierung statischer Attribute

FDP_RIP.1: Teilweiser Schutz bei erhalten gebliebenen Informationen
Ist hierarchisch zu: Keinen anderen Komponenten.

FDP_RIP.1.1:
Die TSF müssen sicherstellen, daß der frühere Informationsinhalt eines Betriebsmittels bei **Wiederfreigabe eines Betriebsmittels von** *folgenden Objekten:* **OB.PIN (Identifikationsdaten)** *nicht verfügbar ist.*

Verfeinerung:
Eine Speicheraufbereitung des Buffers zur Übertragung der PIN (OB.PIN) vom Keypad zur Chipkarte erfolgt im Rahmen der sicheren PIN-Eingabe (SF.PINCMD) nach Übertragung des Kommandos an die Chipkarte (auch bei Kommunikationsfehlern oder zwischenzeitlich gezogener Karte), bei Abbruch durch den Anwender und bei einem Timeout während der PIN-Eingabe.

Abhängigkeiten:
Keine Abhängigkeiten

FTP_TRP.1: Vertrauenswürdiger Pfad
Ist hierarchisch zu: Keinen anderen Komponenten.

FTP_TRP.1.1:
Die TSF müssen einen Kommunikationspfad zwischen sich und **lokalen** *Benutzern bereitstellen, der logisch von den anderen Kommunikationspfaden getrennt ist und eine gesicherte Identifikation seiner Endpunkte* **(Verfeinerung: durch eine optische Anzeige (orangefarbene LED))** *sowie den Schutz der Kommunikationsdaten vor Modifizierung oder Preisgabe bereitstellt.*

FTP_TRP.1.2:
Die TSF müssen **den TSF** *erlauben, eine Kommunikation über den vertrauenswürdigen Pfad einzuleiten.*

FTP_TRP.1.3:
Die TSF müssen den Gebrauch des vertrauenswürdigen Pfads für **die sichere PIN-Eingabe** *erfordern.*

Abhängigkeiten:
Keine Abhängigkeiten

FPT_PHP.1: Passive Erkennung materieller Angriffe
Ist hierarchisch zu: Keinen anderen Komponenten.

FPT_PHP.1.1:
Die TSF müssen materielle Manipulationen **(Verfeinerung: Öffnen des Gehäuses)** *, die die TSF bloßstellen können, eindeutig erkennen.*

FPT_PHP.1.2:
Die TSF müssen die Fähigkeit zum Feststellen erfolgter materieller Manipulationen **(Verfeinerung: Beschädigung der Versiegelung)** *der TSF-Geräte oder TSF-Elemente bereitstellen.*

Abhängigkeiten:
Keine Abhängigkeiten[2]

FPT_PHP.3: Widerstand gegen materielle Angriffe
Ist hierarchisch zu: Keinen anderen Komponenten.

FPT_PHP.3.1:
Die TSF müssen **dem Versuch des Download nicht authentischer Firmware als Szenario der materiellen Manipulation** *von* **aktueller Firmware des EVG** *widerstehen, indem diese automatisch so reagieren, daß die TSP nicht verletzt wird.*

Abhängigkeiten:
Keine Abhängigkeiten

[2] Anmerkung: Die Abhängigkeit von FMT_MOF.1 wurde in Final Interpretation #212 entfernt

FDP_ETC.1 Export von Benutzerdaten ohne Sicherheitsattribute
Ist hierarchisch zu: Keinen anderen Komponenten.

FDP_ETC.1.1:
Die TSF müssen die **Chipkartenleser-Zugriffspolitik** *bei Export von unter Kontrolle der SFPs stehenden Benutzerdaten nach außerhalb des TSC durchsetzen.*

FDP_ETC.1.2:
Die TSF müssen die Benutzerdaten ohne die mit ihnen verknüpften Sicherheitsattribute exportieren.

Abhängigkeiten:
[FDP_ACC.1 Teilweise Zugriffskontrolle, oder
FDP_IFC.1 Teilweise Informationsflußkontrolle]

FDP_UCT.1 Einfache Vertraulichkeit des Datenaustausches
Ist hierarchisch zu: Keinen anderen Komponenten.

FDP_UCT.1.1:
Die TSF müssen die **Chipkartenleser-Zugriffspolitik** *durchsetzen, um in der Lage zu sein, Objekte vor nichtautorisierter Preisgabe geschützt zu* **empfangen**.

Abhängigkeiten:
[FTP_ITC.1 Inter-TSF Vertrauenswürdiger Kanal, oder
FTP_TRP.1 Vertrauenswürdiger Pfad]
[FDP_ACC.1 Teilweise Zugriffskontrolle, oder
FDP_IFC.1 Teilweise Informationsflußkontrolle]

5.2. Anforderungen an die Vertrauenswürdigkeit des TOE (EVG)

Die Anforderungen für den angestrebten Evaluation Assurance Level 3 sind in Tabelle 6.4 Common Criteria Teil 3 wie folgt dargestellt:

Vertrauenswürdigkeitsklasse	Vertrauenswürdigkeitskomponenten
Konfigurationsmanagement	**ACM_CAP.3 Autorisierungskontrolle**
	ACM_SCP.1 EVG-CM-Umfang
Auslieferung und Betrieb	ADO_DEL.1 Auslieferungsprozeduren
	ADO_IGS.1 Installations-, Generierungs- und Anlaufprozeduren
Entwicklung	ADV_FSP.1 Informelle funktionale Spezifikation
	ADV_HLD.2 Sicherheitsspezifischer Entwurf auf hoher Ebene
	ADV_RCR.1 Informeller Nachweis der Übereinstimmung
Handbücher	AGD_ADM.1 Systemverwalterhandbuch
	AGD_USR.1 Benutzerhandbuch
Lebenszyklus-Unterstützung	**ALC_DVS.1 Identifikation der Sicherheitsmaßnahmen**
Testen	**ATE_COV.2 Analyse der Testabdeckung**
	ATE_DPT.1 Testen - Entwurf auf hoher Ebene
	ATE_FUN.1 Funktionales Testen
	ATE_IND.2 Unabhängiges Testen – Stichprobenartig
Schwachstellenbewertung	**AVA_MSU.1 Prüfung der Handbücher**
	AVA_SOF.1 Stärke der EVG-Sicherheitsfunktionen
	AVA_VLA.1 Schwachstellenanalyse des Entwicklers

Darüber hinaus werden aufgrund SigG/SigV [6], [7] die folgenden Anforderungen an die Vertrauenswürdigkeit des EVG gestellt:

- **ADO_DEL.2: Erkennung von Modifizierungen (ersetzt ADO_DEL.1)**
- **ADV_IMP.1: Teilmenge der Implementierung der TSF**
- **ADV_LLD.1: Beschreibender Entwurf auf niedriger Ebene**
- **ALC_TAT.1: Klar festgelegte Entwicklungswerkzeuge**
- **AVA_MSU.3: Analysieren und Testen auf unsichere Zustände (ersetzt AVA_MSU.1)**
- **AVA_VLA.4: Hohe Widerstandsfähigkeit: (ersetzt AVA_VLA.1)**

5.3. Sicherheitsanforderungen an die IT-Umgebung

FDP_RIP.1_SSEE: Teilweiser Schutz bei erhalten gebliebenen Informationen
Ist hierarchisch zu: Keinen anderen Komponenten.

FDP_RIP.1_SSEE.1:
Die **SF der IT-Umgebung (SSEE)** *müssen sicherstellen, daß der frühere Informationsinhalt eines Betriebsmittels bei* **Wiederfreigabe eines Betriebsmittels von** *folgenden Objekten***:**
OB.PIN (Identifikationsdaten) *nicht verfügbar ist.*

Abhängigkeiten:
Keine Abhängigkeiten

6. EVG-Übersichtsspezifikation „ASE_TSS.1“

6.1. EVG-Sicherheitsfunktionen

SF.PINCMD:

Die Firmware im Lesegerät prüft die Kommandos an den Chipkartenleser anhand ihrer Kommandostruktur gemäß CCID [8] bzw. CT-BCS [2]. Werden diese Kommandos als solche zum Verifizieren bzw. Modifizieren der PIN erkannt und ist ein an die Chipkarte weiterzuleitendes Kommando mit einem der folgenden Instruction-Bytes enthalten:

- VERIFY (ISO/IEC 7816-4): INS=0x20
- CHANGE REFERENCE DATA (ISO/IEC 7816-8): INS=0x24
- ENABLE VERIFICATION REQUIR EMENT (ISO/IEC 7816-8): INS=0x28
- DISABLE VERIFICATION REQUIREMENT (ISO/IEC 7816-8): INS=0x26
- RESET RETRY COUNTER (ISO/IEC 7816-8): INS=0x2C
- UNBLOCK APPLICATION (EMV2000): INS=0x18

wird in den Modus zur sicheren Erfassung der PIN über das integrierte Keypad geschaltet.

Die RS232- und die USB-Variante des EVG unterscheiden sich lediglich im Protokoll-Anbindungs-Modul an den Host, so dass bei beiden Host-Interface Varianten ein identischer Datenstrom durch die Sicherheitsfunktion bearbeitet wird.

Die Sicherheitsfunktion SF.PINCMD erkennt die von der Host-Software übermittelten Kommandos zur PIN-Eingabe und fügt die über das Keypad eingegebenen Nummern als PIN an die entsprechenden Stellen des Kommandos an die Chipkarte ein. Dabei wird nur die Tatsache an den Host gemeldet, dass eine der numerischen Tasten gedrückt wurde.Der Benutzer kann die Eingabe der PIN mit der (roten) Abbruchtaste jederzeit abbrechen, wodurch die Übertragung der PIN zur Chipkarte verhindert wird. Je nach Kommando-Ausprägung nach CCID[8] bzw. CT-BCS[2] muss der Benutzer die Eingabe der PIN mit der (grünen) Bestätigungstaste abschliessen (alternativ kann die PIN-Länge vorgegeben werden, so dass die letzte Ziffer der PIN die Eingabe abschliesst). Der Summer ist durch den Benutzer abschaltbar und somit nicht Teil der Sicherheitsleistung des EVG.

Dies dient der Host-Applikation, um dem Anwender mit „*“ den Eingabefortschritt anzuzeigen. Während der PIN-Eingabe zeigen die entsprechenden LEDs den sicheren Eingabemodus an.

SF.CLMEM:

Die Speicherbereiche für die PIN-Daten werden im Rahmen der sicheren PIN-Eingabe (SF.PINCMD) nach Übertragung des Kommandos an die Chipkarte (auch bei Kommunikationsfehlern oder zwischenzeitlich gezogener Karte), bei Abbruch durch den Anwender und bei einem Timeout während der PIN-Eingabe wiederaufbereitet. Nach der Wiederaufbereitung ist die PIN nicht mehr im Speicher des EVG vorhanden.

SF.SECDOWN:

Eine neue Firmware kann in den EVG eingespielt werden. Dazu wird der EVG in den Bootloader-Modus versetzt, in dem alle Funktionen des EVG deaktiviert werden, bis auf die Entgegennahme einer neuen Firmware, die mit einer elektronischen Signatur des Herstellers versehen ist. Aus dem Bootloader-Modus kann nur eine neu entgegengenommene, korrekt signierte Firmware (s.u.) wieder aktiviert werden, eine Rückkehr zur vormals installierten Firmware ist nicht mehr möglich. Eine entgegengenommene Firmware mit fehlerhafter Signatur wird nicht aktiviert, sondern es wird wieder in den Bootloader-Modus verzweigt, der wiederum auf eine neue Firmware wartet.

Die Verifikation einer Signatur der Firmware mit dem asymmetrischen ECDSA-Algorithmus und einer Bitlänge von 192 garantiert die Integrität und Authentizität der Firmware beim Laden einer neuen Firmware in den Chipkartenleser.Der Hash-Wert über die neu zu ladende Firmware wird basierend auf dem Algorithmus SHA-1 mit einer Länge von 160 Bit ermittelt.

Die Verifikation der Integrität und Authentizität erfolgt im EVG durch Vergleich des ermittelten Hash-Wertes und des Hash-Wertes als Bestandteil der entschlüsselten Signatur. Der öffentliche Schlüssel ist hierfür im EVG gespeichert.

SF.SEAL:

Das Gehäuse des EVG ist durch eine Versiegelung so verschlossen, dass es ohne eine Beschädigung der Versiegelung nicht geöffnet werden kann. Die Versiegelung ist so beschaffen, dass eine Ablösung vom Untergrund (also vom Gehäuse) nicht ohne erkennbare Beschädigung der Versiegelung möglich ist.

Hersteller der Siegel:	Firma Trautwein Security
Fabrikat:	SicoTra

Die Siegel sind als „Sicherheitsetiketten“ evaluiert durch das BSI nach Sicherheitsstufe 2. Nachzulesen in [9].

Der Kunde wird in der Benutzerdokumentation belehrt, die Unversehrtheit der Versiegelung vor jeder PIN-Eingabe zu kontrollieren und das Gerät im Falle einer beschädigten Versiegelung nicht weiter zu benutzen.

Durch organisatorische und vertragliche Massnahmen ist sichergestellt, dass die Siegel nur im Rahmen der regulären Produktion von KOBIL Chipkartenterminals eingesetzt werden und Dritten nicht zur Verfügung stehen.

Die Sicherheitsfunktion SF.SECDOWN beruht auf kryptographischen Wahrscheinlichkeits-Mechanismen. SF.SEAL basiert auf einem Mechanismus der mechanischen Versiegelung, die hohem Angriffspotential widersteht.

6.2. Maßnahmen zur Vertrauenswürdigkeit

Die Maßnahmen zur Vertrauenswürdigkeit werden durch folgende Dokumente des Herstellers reflektiert.

- Konfigurationsmanagement
- Auslieferung und Betrieb
- Entwicklung:
  - Informelle funktionale Spezifikation
  - Sicherheitsspezifischer Entwurf auf hoher Ebene
  - Darstellung der Implementierung
  - Entwurf auf niedriger Ebene
  - Informeller Nachweis der Übereinstimmung
- Benutzerhandbuch
- Lebenszyklus-Unterstützung / Identifikation der Sicherheitsmaßnahmen
- Testdokumentation
- Schwachstellenbewertung

7. PP-Postulate „ASE_PPC.1“

Es wird keine Erfüllung eines PP durch die vorliegenden Sicherheitsvorgaben angestrebt

8. Erklärung

8.1. Erklärung der Sicherheitsziele

Zusammenhänge: Annahmen, Bedrohungen - Sicherheitsziele

	Annahmen	**Sicherheitsziele**	**Kommentar**
A1	A.USER.RESP1	OE.USER.RESP1	Durch die Formulierung der Annahmen und Ziele ist die Korrespondenz gegeben.
A2	A.USER.RESP2	OE.USER.RESP2	Durch die Formulierung der Annahmen und Ziele ist die Korrespondenz gegeben.
A3	A.USER.RESP3	OE.USER.RESP3	Durch die Formulierung der Annahmen und Ziele ist die Korrespondenz gegeben.
A4	A.USER.RESP4	OE.USER.RESP4	Durch die Formulierung der Annahmen und Ziele ist die Korrespondenz gegeben.
A5	A.USER.RESP5	OE.USER.RESP5	Durch die Formulierung der Annahmen und Ziele ist die Korrespondenz gegeben.
A6	A.USER.RESP6	OE.USER.RESP6	Durch die Formulierung der Annahmen und Ziele ist die Korrespondenz gegeben.
A7	A.USER.RESP7	OE.USER.RESP7	Durch die Formulierung der Annahmen und Ziele ist die Korrespondenz gegeben.

	Bedrohung	Sicherheitsziele	Kommentar
T1	T.REVEAL.1	O.REVEAL O.STORE	Der EVG garantiert, dass die PIN den Leser nicht in Richtung Host verlässt, sie wird nicht dauerhaft im EVG gespeichert.
T2	T.REVEAL.2	O.MODE O.REVEAL O.STORE OE.USER.RESP2 OE.USER.RESP6	Der EVG zeigt den Modus der sicheren PIN-Eingabe durch eine LED eindeutig an Der EVG garantiert, dass die PIN den Leser nicht in Richtung Host verlässt, diese wird im EVG nicht dauerhaft gespeichert und ist somit nicht ausserhalb der SSEE verfügbar Der Endawender muss während der PIN-Eingabe mittels der LEDs verifizieren, dass sich der Leser im Modus der sicheren PIN-Eingabe befindet. Es werden für qualifizierte Signaturen nur bestätigte Signatur-Chipkarten eingesetzt, welche die PIN nicht preisgeben.
T3	T.STORE.1	O.STORE	Der EVG speichert dauerhaft keine Identifikationsdaten.
T4	T.MODIFY.1	O.MODIFY_DLD OE.USER.RESP3	Das sichere Firmware-Download des EVG garantiert, dass der EVG nicht unautorisiert verändert werden kann. Der Endanwender prüft vor der Installation einer neuen Firmware, ob diese bestätigt und zertifiziert ist
T5	T.MODIFY.2	O.MODIFY_SEAL OE.USER.RESP4	Die Versiegelung zeigt einen Manipulationsversuch an der Hardware des EVG an Der Endanwender kann am Zustand der Versiegelung erkennen, dass keine Manipulationen an der Hardware vorgenommen wurden.

Das Sicherheitsziel O.REVEAL wirkt gegen Bedrohung T.REVEAL.1 und T.REVEAL.2, da die Weitergabe der PIN ausschliesslich im Rahmen eines zulässigen Kommandos und nur an die Signatur-Chipkarte erfolgt.

Das Sicherheitsziel O.MODE wirkt gegen Bedrohung T.REVEAL.2, da die Anzeige des Modus der sicheren PIN Eingabe (über die orangefarbene LED) den Benutzer davon abhält, die PIN zu einem Zeitpunkt einzugeben, an dem die Eingabe vom PC aus lesbar wäre. Das Sicherheitsziel OE.USER.RESP2 legt dieses Verhalten in die Verantwortung des Benutzers, genauso wie OE.USER.RESP6 sicherstellt, dass nur bestätigte Signatur-Chipkarten zum Einsatz kommen, welche ihrerseits die PIN nicht preisgeben.

Das Sicherheitsziel O.STORE wirkt gegen Bedrohung T.STORE, T.REVEAL.1 und T.REVEAL.2, da die nicht stattfindende dauerhafte Speicherung der Identifikationsdaten im EVG ein späteres Auslesen derselben ausschließt.

Das Sicherheitsziel O.MODIFY_DLD wirkt gegen Bedrohung T.MODIFY.1, da keine unauthorisierte Veränderung der Firmware in den EVG über die Update-Funktion eingebracht werden kann und der Benutzer gemäß OE.USER.RESP3 nur bestätigte und zertifizierte Komponenten installiert.

Das Sicherheitsziel O.MODIFY_SEAL wirkt gegen Bedrohung T.MODIFY.2, da eine physikalische Manipulation am EVG für den Benutzer sichtbar wird, und es gemäß OE.USER.RESP4 in seiner Verantwortung liegt, den EVG in diesem Fall nicht mehr zu benutzen.

Querverweise: Bedrohungen - Sicherheitsziele des EVG

	O.REVEAL	O.MODE	O.STORE	O.MODIFY_DLD	O.MODIFY_SEAL
T.REVEAL.1	✓		✓		
T.REVEAL.2	✓	✓	✓		
T.STORE.1			✓		
T.MODIFY.1				✓	
T.MODIFY.2					✓

Querverweise: Annahmen/Bedrohungen - Sicherheitsziele der Umgebung

	OE. USER. RESP1	OE. USER. RESP2	OE. USER. RESP3	OE. USER. RESP4	OE. USER. RESP5	OE. USER. RESP6	OE. USER. RESP7
A.USER. RESP1	✓						
A.USER. RESP2		✓					
A.USER. RESP3			✓				
A.USER. RESP4				✓			
A.USER. RESP5					✓		
A.USER. RESP6						✓	
A.USER. RESP7							✓
T.REVEAL.1							
T.REVEAL.2		✓				✓	
T.STORE.1							
T.MODIFY.1			✓				
T.MODIFY.2				✓			

8.2. Erklärung der Sicherheitsanforderungen

Die Mindeststärke der Funktionen „SOF-hoch“ wird von SigV [7], Anhang 1, Ziffer 1.2 gefordert und ist somit angemessen und konsistent mit den Sicherheitszielen des EVGs.

Die in FCS_COP.1_ECDSA und FCS_COP.1_SHA verwendeten Parameter und Schlüssellängen entsprechen der Mechanismen-Stärke „SOF-hoch“, wie SigG-Alg[12] zu entnehmen ist.

Die Mindeststärke der Funktionen „SOF-hoch“ ist den Anforderungen an die Vertrauenswürdigkeit angemessen, was sich in den über EAL3 hinausgehenden Anforderungen

- ADO_DEL.2 (Erkennung von Modifizierungen)
- ADV_IMP.1 (Teilmenge der Implementierung der TSF)
- ADV_LLD.1 (Beschreibender Entwurf auf niedriger Ebene)
- ALC_TAT.1 (Klar festgelegte Entwicklungswerkzeuge)
- AVA_MSU.3 (Analysieren und Testen auf unsichere Zustände)
- AVA_VLA.4 (Hohe Widerstandsfähigkeit)

widerspiegelt.

Die Menge der gewählten Sicherheitsanforderungen bilden ein sich gegenseitig unterstützendes und in sich konsistentes Ganzes, da alle relevanten Abhängigkeiten berücksichtigt werden.

Zusammenhänge: IT-Sicherheitsziele - Sicherheitsanforderungen

	Sicherheits-Ziele	**Sicherheits-anforderungen**	**Kommentar**
O1	O.REVEAL	FDP_ACC.1 FDP_ACF.1 FTP_TRP.1 FDP_UCT.1 FDP_ETC.1	Die Ablaufsteuerung zur „Sicheren PIN-Eingabe“ garantiert, dass nur zugelassene Kommandos an die Chipkarte weitergeleitet werden und verhindert damit, dass der Benutzer die PIN eingibt, während die Tastatur vom Host auslesbar ist. Die PIN wird über die einzig verfügbare Eingabeschnittstelle zum Benutzer (die Tastatur) entgegengenommen und die Chipkartenleser-Zugriffspolitik durchgesetzt
O2	O.MODE	FTP_TRP.1	Die LEDs des EVG zeigen den Modus der „Sicheren PIN-Eingabe“ an
O3	O.STORE	FDP_RIP.1	Eine Speicheraufbereitung des Buffers zur Übertragung der PIN vom Keypad zur Chipkarte erfolgt im Rahmen der sicheren PIN-Eingabe (SF.PINCMD) nach Übertragung des Kommandos an die Chipkarte (auch bei Kommunikationsfehlern oder zwischenzeitlich gezogener Karte), bei Abbruch durch den Anwender und bei einem Timeout während der PIN-Eingabe.
O4	O.MODIFY_DLD	FCS_COP.1_ECDSA FCS_COP.1_SHA	Die Verifikation einer Signatur der Firmware mit dem Hash-Algorithmus SHA-1 und dem asymmetrischen ECDSA-Algorithmus mit einer Bitlänge von 192 garantiert die Integrität und Authentizität der Firmware beim Laden der Firmware

			in den Chipkartenleser.
		FPT_PHP.3	Die Absicherung des Firmware-Downloads garantiert, dass nur authentische Firmware im EVG zur Ausführung kommen kann.
		ACM_CAP.3	Die Firmware des EVG ist eindeutig gekennzeichnet, der Hersteller hat ein Konfigurationsmanagement dafür
		ADO_DEL.2	Die ausgelieferte signierte Firmware des EVG ist authentisch
		ALC_DVS.1	Die Sicherheit in der Entwicklung ist gewährleistet
O5	O.MODIFY_SEAL	FPT_PHP.1	Die Versiegelung garantiert die Erkennbarkeit von Manipulationen am EVG
		ACM_CAP.3	Die Versiegelung unterliegt einer Verwaltung beim Hersteller
		ADO_DEL.2	Der Versiegelte EVG ist bei Auslieferung nicht materiell manipuliert
O6	OE.USER.RESP6	FDP_RIP.1_SSEE	Die Signatur-Chipkarte (mit der der EVG betrieben wird) muss evaluiert und bestätigt sein. Damit ist sichergestellt, dass sie die Identifikationsdaten nicht speichert.

Querverweise: IT-Sicherheitsziele- Sicherheitsanforderungen

	O.REVEAL	O.MODE	O.STORE	O.MODIFY_DLD	O.MODIFY_SEAL	OE.USER.RESP6
FDP_ACC.1	✓					
FDP_ACF.1	✓					
FDP_ETC.1	✓					
FDP_UCT.1	✓					
FTP_TRP.1	✓	✓				
FDP_RIP.1			✓			
FCS_COP.1_ECDSA				✓		
FCS_COP.1_SHA				✓		
FPT_PHP.3				✓		
FPT_PHP.1					✓	
ACM_CAP.3				✓	✓	
ADO_DEL.2				✓	✓	
ALC_DVS.1				✓		
FDP_RIP.1_SSEE						✓

Das Anforderungselement **FDP_ACC.1.1** trägt zum Sicherheitsziel **O.REVEAL** bei, da die Zugriffskontrolle auf dem Objekt OB.PIN (= Identifikationsdaten) über die Operationen OP.P_ENTRY (=Eingabe der PIN) und OP.P_CMD (Kommando-Template vom PC) definiert wird. Die teilweise Zugriffskontrolle ist ausreichend, weil die Operation zur Speicheraufbereitung für die Durchsetzung des Sicherheitsziels nicht kontrolliert werden muß.

Das Anforderungselement **FDP_ACF.1.1** trägt zum Sicherheitsziel **O.REVEAL** bei, da die Objekte nur über definierte Schnittstellen des EVG's erreichbar sind und je Schnittstelle nur ein Subjekt definiert ist (S.USER -> Tastatur, S.PC -> Host PC). Der Verzicht auf die Verwendung von Sicherheitsattributen entspricht dem Sicherheitsziel.

Das Anforderungselement **FDP_ACF.1.2** trägt zum Sicherheitsziel **O.REVEAL** bei, da die Kommando-Templates in OP.P_CMD auf ihre Unbedenklichkeit hinsichtlich der Preisgabe der Identitifkationsdaten geprüft werden und der Benutzer bei OP.P_ENTRY die Möglichkeit zum Abbruch der PIN (OB.PIN) Eingabe hat.

Die Anforderungselemente **FDP_ACF.1.3** und **FDP_ACF.1.4** tragen zum Sicherheitsziel **O.REVEAL** bei, da keine Authorisierung oder Regel-basierte Verweigerung beim Zugriff erlaubt ist.

Das Anforderungselement **FDP_ETC.1.1** trägt zum Sicherheitsziel **O.REVEAL** bei, da die Chipkartenleser-Zugriffspolitik durchgesetzt wird.

Das Anforderungselement **FDP_ETC.1.2** trägt zum Sicherheitsziel **O.REVEAL** bei, da keine Sicherheitsattribute mit dem Objekt OB.PIN verknüpft sind.

Das Anforderungselement **FDP_UCT.1.1** trägt zum Sicherheitsziel **O.REVEAL** bei, da die Chipkartenleser-Zugriffspolitik durchgesetzt wird.

Das Anforderungselement **FTP_TRP.1.1** trägt zum Sicherheitsziel **O.REVEAL** bei, da die Identifikationsdaten beim Empfang vor Preisgabe geschützt werden.

Das Anforderungselement **FTP_TRP.1.2** trägt zum Sicherheitsziel **O.REVEAL** bei, da die Identifikationsdaten beim Empfang vor Preisgabe geschützt werden.

Das Anforderungselement **FTP_TRP.1** trägt zum Sicherheitsziel **O.REVEAL** bei, weil der von **FDP_UCT.1** geforderte geschützte Empfang durch die Verwendung eines vertrauenswürdigen Pfades für die sichere PIN-Eingabe (**FTP_TRP.1.3**) von einem lokalen Benutzer (**FTP_TRP.1.1**) realisiert werden soll. Die Trennung von anderen Kommunikationspfaden (**FTP_TRP.1.1**) in Verbindung mit der Einleitung der Kommunikation durch die TSF (**FTP_TRP.1.2**) gewährleistet den Schutz der Identifikationsdaten vor Preisgabe (an den Host).

Das Anforderungselement **FTP_TRP.1.1** trägt zum Sicherheitsziel **O.MODE** bei, da der Kommunikationspfad logisch von anderen Kommunikationspfaden getrennt ist und dessen Endpunkt – die orangefarbene LED - sicher identifiziert werden kann.

Das Anforderungselement **FTP_TRP.1.3** trägt zum Sicherheitsziel **O.MODE** bei, da der Modus der „sicheren PIN Eingabe" durch einen vertrauenswürdigen Pfad realisiert wird.

Das Anforderungselement **FDP_RIP.1.1** trägt zum Sicherheitsziel **O.STORE** bei, da nach der Wiederfreigabe des Betriebsmittels „Kommando-Puffer" die Identifikationsdaten gelöscht werden, so dass diese nicht dauerhaft ausserhalb des für die Verarbeitung unbedingt notwendigen Zeitraums (festgelegt durch die Verfeinerung) gespeichert sind.

Das Anforderungselement **FCS_COP.1_ECDSA.1** trägt zum Sicherheitsziel **O.MODIFY_DLD** bei, da der kryptographische Mechanismus „ECDSA Signatur mit 192 Bit Schlüssel-Länge“ authorisierte Software-Aktualisierungen erkennbar macht und somit ein gesichertes Software-Update ermöglicht.

Das Anforderungselement **FCS_COP.1_SHA.1** trägt zum Sicherheitsziel **O.MODIFY_DLD** bei, da der kryptographische Mechanismus „SHA.1“ authorisierte Software-Aktualisierungen erkennbar macht und somit ein gesichertes Software-Update ermöglicht.

Das Anforderungselement **FPT_PHP.3.1** trägt zum Sicherheitsziel **O.MODIFY_DLD** bei, da als nicht-authentisch betrachtete Software-Updates abgelehnt werden.

Das Anforderungselement **ACM_CAP.3** trägt zum Sicherheitsziel **O.MODIFY_DLD** bei, da die Firmware beim Hersteller einem Konfigurationsmanagement unterliegt und eindeutig gekennzeichnet ist.

Das Anforderungselement **ADO_DEL.2** trägt zum Sicherheitsziel **O.MODIFY_DLD** bei, da der Hersteller dafür sorgt, dass die ausgelieferte Firmware authentisch ist.

Das Anforderungselement **ALC_DVS.1** trägt zum Sicherheitsziel **O.MODIFY_DLD** bei, da der Hersteller für die Sicherheit in der Entwicklungsumgebung sorgt.

Das Anforderungselement **FPT_PHP.1.1** trägt zum Sicherheitsziel **O.MODIFY_SEAL** bei, da materielle Manipulationen (Öffnen des Gehäuses) an der Versiegelung des EVG durch Beschädigung derselben erkannt werden.

Das Anforderungselement **FPT_PHP.1.2** trägt zum Sicherheitsziel **O.MODIFY_SEAL** bei, da eine beschädigte Versiegelung für den Benutzer erkennbar ist.

Das Anforderungselement **ACM_CAP.3** trägt zum Sicherheitsziel **O.MODIFY_SEAL** bei, da die Versiegelung beim Hersteller des EVG der Lagerverwaltung unterliegt, die den Bestand genau kontrolliert.

Das Anforderungselement **ADO_DEL.2** trägt zum Sicherheitsziel **O.MODIFY_SEAL** bei, da der Hersteller dafür sorgt, dass der versiegelte EVG bei der Auslieferung nicht materiell manipuliert ist.

Das Anforderungselement **FDP_RIP.1_SSEE.1** trägt zum Sicherheitsziel **OE.USER.RESP6** bei, da die PIN (OB.PIN) nach der Verarbeitung in der SSEE gelöscht wird.

Abhängigkeiten der funktionalen Sicherheitsanforderungen

	Sicherheits-Anforderungen	Abhängigkeiten	Referenz
SFR1	FCS_COP.1_ECDSA	[FDP_ITC.1 oder FDP_ITC.2 oder FCS_CKM.1] FCS_CKM.4 FMT_MSA.2	nicht zutreffend nicht zutreffend nicht zutreffend nicht zutreffend nicht zutreffend
SFR2	FCS_COP.1_SHA	[FDP_ITC.1 oder FDP_ITC.2 oder FCS_CKM.1] FCS_CKM.4 FMT_MSA.2	nicht zutreffend nicht zutreffend nicht zutreffend nicht zutreffend nicht zutreffend
SFR3	FDP_ACC.1	FDP_ACF.1	SFR4
SFR4	FDP_ACF.1	FDP_ACC.1 FMT_MSA.3	SFR3 nicht zutreffend
SFR5	FDP_RIP.1	Keine	-
SFR6	FTP_TRP.1	Keine	-
SFR7	FPT_PHP.1	Keine[3]	-
SFR8	FPT_PHP.3	Keine	-
SFR9	FDP_ETC.1	[FDP_ACC.1 oder FDP_IFC.1]	SFR3 -
SFR10	FDP_UCT.1	[FTP_ITC.1 oder FTP_TRP.1] [FDP_ACC.1 oder FDP_IFC.1]	- SFR6 SFR3 -
SFR11	FDP_RIP.1_SSEE	Keine	-

SFR1: FCS_COP.1_ECDSA

FDP_ITC.1 oder FDP_ITC.2

- *Import von Benutzerdaten ohne/mit Sicherheitsattribute(n)*
- Ist eine Anforderung für die Entwicklungsumgebung des Herstellers den Import des Öffentlichen Schlüssels beschreibend
- Keine unmittelbare Abhängigkeit für den EVG, da der Schlüssel beim Hersteller eingebracht und mit dem EVG ausgeliefert wird

FCS_CKM.1

- *Kryptographische Schlüsselgenerierung*
- Ist eine Anforderung für die Entwicklungsumgebung des Herstellers die Schlüsselgenerierung beschreibend
- Keine unmittelbare Abhängigkeit für den EVG

FCS_CKM.4

- *Zerstörung des kryptographischen Schlüssels*
- Ist eine Anforderung an die Entwicklungs-Umgebung die Zerstörung des generierten privaten Schlüssel beschreibend
- Keine unmittelbare Abhängigkeit für den EVG, da dieser nur den öffentlichen Schlüssel enthält

[3] Anmerkung: Die Abhängigkeit von FMT_MOF.1 wurde in Final Interpretation #212 entfernt

FMT_MSA.2

- *Sichere Sicherheitsattribute*
- Der EVG hat keinen Einfluß auf die Akzeptanz sicherer Werte für die Sicherheitsattribute kryptographischer Schlüssel, weil diese als integraler Bestandteil des EVG anzusehen sind und bereits bei der Herstellung eingebracht werden.

SFR2: FCS_COP.1_SHA

FDP_ITC.1 oder FDP_ITC.2

- *Import von Benutzerdaten ohne/mit Sicherheitsattribute(n)*
- Keine Abhängigkeit, da der Hash-Algorithmus keine Schlüssel verwendet

FCS_CKM.1

- *Kryptographische Schlüsselgenerierung*
- Keine Abhängigkeit, da der Hash-Algorithmus keine Schlüssel verwendet

FCS_CKM.4

- *Zerstörung des kryptographischen Schlüssels*
- Keine Abhängigkeit, da der Hash-Algorithmus keine Schlüssel verwendet

FMT_MSA.2

- *Sichere Sicherheitsattribute*
- Keine Abhängigkeit, da der Hash-Algorithmus keine Schlüssel verwendet

SFR3: FDP_ACC.1

FDP_ACF.1

- *Zugriffskontrolle basierend auf Sicherheitsattributen*
- Siehe FDP_ACF.1

SFR4: FDP_ACF.1

FDP_ACC.1

- *Teilweise Zugriffskontrolle*
- Siehe FDP_ACC.1

FMT_MSA.3

- *Initialisierung statischer Attribute*
- An die Initialisierung statischer Attribute ist keine Anforderung zu stellen, weil die Chipkartenleser-Zugriffspolitik auf keinen Attributen basiert

SFR6: SFR5: FDP_RIP.1

Keine Abhängigkeiten

SFR6: FTP_TRP.1

Keine Abhängigkeiten

SFR7: FPT_PHP.1

Keine Abhängigkeiten[4]

SFR8: FPT_PHP.3

Keine Abhängigkeiten

SFR9: FDP_ETC.1

FDP_ACC.1

- *Teilweise Zugriffskontrolle*
- Siehe FDP_ACC.1

SFR10: FDP_UCT.1

FDP_ACC.1

- *Teilweise Zugriffskontrolle*
- Siehe FDP_ACC.1

FTP_TRP.1

- *Vertrauenswürdiger Pfad*
- Siehe FTP_TRP.1

SFR11: FDP_RIP.1_SSEE

Keine Abhängigkeiten

[4] Anmerkung: Die Abhängigkeit von FMT_MOF.1 wurde in Final Interpretation #212 entfernt

8.3. Erklärung der EVG-Übersichtsspezifikation

Die Sicherheitsfunktionen SF.PINCMD und SF.CLMEM zur sicheren PIN-Eingabe einschließlich LED-Steuerung und Speicheraufbereitung sind aufgrund ihrer Implementierungen nicht direkt angreifbar.

Für die Sicherheitsfunktionen SF.SECDOWN und SF.SEAL[5] wird die Stärke „SOF-hoch“ gefordert. Dies ist konsistent mit der geforderten Mindeststärkestufe.

Sicherheitsanforderungen und Sicherheitsfunktionen
Die nachfolgend dargestellten Sicherheitsfunktionen ergänzen sich und entsprechen in ihrem Zusammenwirken den Sicherheitsanforderungen des EVGs. Wie zu erkennen ist, wird jede Sicherheitsanforderung von jeweils einer einzelnen Sicherheitsfunktion erfüllt. Alle Sicherheitsanforderungen werden durch die vorhandenen Sicherheitsfunktionen, die sich gegenseitig zu einem sicheren Gesamtsystem ergänzen, abgedeckt.

	Sicherheits-Funktion	**Sicherheits-anforderungen**	**Kommentar**
SF1	SF.PINCMD	FDP_ACC.1 FDP_ACF.1 FTP_TRP.1 FDP_UCT.1 FDP_ETC.1	Die Sicherheitsfunktion garantiert, dass nur zugelassene Kommandos an die Chipkarte weitergeleitet werden. Die LEDs des Lesers zeigen den Modus der „Sicheren PIN-Eingabe“ über einen vertrauenswürdigen Pfad an. Die PIN wird vom Benutzer über die Tastatur entgegengenommen und an die Chipkarte exportiert.
SF2	SF.CLMEM	FDP_RIP.1	Eine Speicheraufbereitung des Buffers zur Übertragung der PIN vom Keypad zur Chipkarte erfolgt im Rahmen der sicheren PIN-Eingabe (SF.PINCMD) nach Übertragung des Kommandos an die Chipkarte (auch bei Kommunikationsfehlern oder zwischenzeitlich gezogener Karte), bei Abbruch durch den Anwender und bei einem Timeout während der PIN-Eingabe.

[5] SF.SEAL ist als „SOF-hoch“ anzusehen, da die mechanische Versiegelung so ausgelegt ist, dass sie einem hohen Angriffspotential widersteht.

SF3	SF.SECDOWN	FCS_COP.1_ECDSA FCS_COP.1_SHA FPT_PHP.3	Die Verifikation einer Signatur der Firmware mit dem Hash-Algorithmus SHA-1 und dem asymmetrischen ECDSA-Algorithmus mit einer Bitlänge von 192 sowie die Ablaufsteuerung garantieren die Integrität und Authentizität der Firmware beim Laden der Firmware in den Chipkartenleser.
SF4	SF.SEAL	FPT_PHP.1	Schutz des Gehäuses vor unbefugter Manipulation

Die Sicherheitsanforderung **FDP_ACC.1.1** wird durch **SF.PINCMD** umgesetzt, da hier die Zugriffskontrolle auf dem Objekt OB.PIN (= Identifikationsdaten) über die Operationen OP.P_ENTRY (=Eingabe der PIN) und OP.P_CMD (Kommando-Template vom PC) vollständig implementiert wird und S_USER das Kommando OP.P_CMD nicht ausführt und S_HOST die Eingabe OP.P_ENTRY nicht ausführt.

Die Sicherheitsanforderung **FDP_ACF.1.1** wird durch **SF.PINCMD** umgesetzt, da in SF.PINCMD keine Sicherheitsattribute verwendet werden, wie in FDP_ACF.1.1 gefordert.

Die Sicherheitsanforderung **FDP_ACF.1.2** wird durch **SF.PINCMD** umgesetzt, da die Kommando-Templates in OP.P_CMD hier auf ihre Unbedenklichkeit hinsichtlich der Preisgabe der Identitifkationsdaten geprüft werden (Positiv-Liste der erlaubten Instruction-Bytes). Der Abbruch der PIN Eingabe (OP.P_ENTRY) durch den Benutzer (S_USER) ist jederzeit möglich.

Die Sicherheitsanforderungen **FDP_ACF.1.3** und **FDP_ACF.1.4** werden durch **SF.PINCMD** umgesetzt, da keine Authorisierung oder Regel-basierte Verweigerung beim Zugriff spezifiziert ist.

Die Sicherheitsanforderung **FDP_ETC.1.1** wird durch **SF.PINCMD** umgesetzt, da der Export des Objekts OB.PIN (=Identifikationsdaten) an die Signatur-Chipkarte unter Kontrolle der Chipkartenleser-Zugriffspolitik hier implementiert ist.

Die Sicherheitsanforderung **FDP_ETC.1.2** wird durch **SF.PINCMD** umgesetzt, da da keine Sicherheitsattribute mit dem Objekt OB.PIN verknüpft sind.

Die Sicherheitsanforderung **FDP_UCT.1.1** wird durch **SF.PINCMD** umgesetzt, da der Empfang des Objekts OB.PIN bei der Eingabe durch S.USER von der Tastatur unter Kontrolle der Chipkartenleser-Zugriffspolitik hier realisiert ist.

Die Sicherheitsanforderung **FTP_TRP.1.1** wird durch **SF.PINCMD** umgesetzt, da der Kommunikationspfad beim Empfang von OB.PIN bei der Eingabe durch S.USER von der Tastatur hier logisch getrennt wird vom Kommunikationspfad zu S.PC. Die Endpunkte (Tastatur, LED) sind über die Schnittstellen klar identifiziert und werden hier entsprechend angesteuert. Die Verfeinerung wird durch die Verwendung der orangefarbenen LED erfüllt.

Die Sicherheitsanforderung **FTP_TRP.1.2** wird durch **SF.PINCMD** umgesetzt, da der Kommunikationspfad hier komplett implementiert ist und durch die IT-Sicherheitsfunktion SF.PINCMD initiiert wird.

Die Sicherheitsanforderung **FTP_TRP.1.3** wird durch **SF.PINCMD** umgesetzt, da hier OB.PIN nur auf dem einen Kommunikationspfad „sichere PIN Eingabe“ von der Tastatur (Eingabe durch S.USER) entgegengenommen wird.

Die Sicherheitsanforderung **FDP_RIP.1.1** wird durch **SF.CLMEM** umgesetzt, da nach der Wiederfreigabe des Betriebsmittels „Kommando-Puffer“ die Identifikationsdaten hier gelöscht werden und damit nicht mehr verfügbar sind.

Die Sicherheitsanforderung **FCS_COP.1_ECDSA.1** wird durch **SF.SECDOWN** umgesetzt, da der kryptographische Mechanismus „ECDSA Signatur mit 192 Bit Schlüssel-Länge“ hier implementiert ist.
Die Sicherheitsanforderung **FCS_COP.1_SHA.1** wird durch **SF.SECDOWN** umgesetzt, da der kryptographische Mechanismus „SHA1“ zur Hashwertbildung hier implementiert ist.

Die Sicherheitsanforderung **FPT_PHP.3.1** wird durch **SF.SECDOWN** umgesetzt, da als „nicht-authentisch“ erkannte Software-Aktualisierungen an dieser Stelle abgelehnt werden und wieder in den Bootloader-Modus verzweigt wird.

Die Sicherheitsanforderung **FPT_PHP.1.1** wird durch **SF.SEAL** umgesetzt, da das Öffnen des Gehäuses als materielle Manipulation am EVG durch Beschädigung von zertifizierten Sicherheitsetiketten (Verfeinerung) erkannt wird.

Die Sicherheitsanforderung **FPT_PHP.1.2** wird durch **SF.SEAL** umgesetzt, da eine beschädigte Versiegelung für den Benutzer erkennbar ist.

Anforderungen und Maßnahmen zur Vertrauenswürdigkeit
Die nachfolgend dargestellten Maßnahmen zur Vertrauenswürdigkeit entsprechen den Anforderungen zur Vertrauenswürdigkeit. Alle Anforderungen zur Vertrauenswürdigkeit werden durch die vorhandenen Maßnahmen zur Vertrauenswürdigkeit, die sich gegenseitig zu einem sicheren Gesamtsystem ergänzen, abgedeckt.

	Maßnahme zur Vertrauens-würdigkeit	**Anforderungen zurVertrauens-würdigkeit**	**Kommentar**
SM1	Konfigurations-management	ACM_CAP.3 ACM_SCP.1	Autorisierungskontrolle EVG-CM-Umfang
SM2	Auslieferung und Betrieb	ADO_DEL.2 ADO_IGS.1	Erkennung von Modifizierungen Installations-, Generierungs- und Anlaufprozeduren
SM3	Informelle funktionale Spezifikation	ADV_FSP.1	Informelle funktionale Spezifikation
SM4	Sicherheitsspezifischer Entwurf auf hoher Ebene	ADV_HLD.2	Sicherheitsspezifischer Entwurf auf hoher Ebene
SM5	Darstellung der Implementierung	ADV_IMP.1	Teilmenge der Implementierung der TSF
SM6	Entwurf auf niedriger Ebene	ADV_LLD.1	Entwurf auf niedriger Ebene

SM7	Informeller Nachweis der Übereinstimmung	ADV_RCR.1	Informeller Nachweis der Übereinstimmung
SM8	Bedienungsanleitung	AGD_ADM.1 AGD_USR.1	Systemverwalterhandbuch Benutzerhandbuch
SM9	Lebenszyklus-Unterstützung / Identifikation der Sicherheitsmaßnahmen	ALC_DVS.1 ALC_TAT.1	Identifikation der Sicherheitsmaßnahmen Klar festgelegte Entwicklungswerkzeuge
SM10	Testdokumentation	ATE_COV.2 ATE_DPT.1 ATE_FUN.1 ATE_IND.2	Analyse der Testabdeckung Testen - Entwurf auf hoher Ebene Funktionales Testen Unabhängiges Testen - Stichprobenartig
SM11	Schwachstellen-bewertung	AVA_MSU.3 AVA_SOF.1 AVA_VLA.4	Analysieren und Testen auf unsichere Zustände Stärke der EVG-Sicherheitsfunktionen Hohe Widerstandsfähigkeit

8.4. Erklärung der PP-Postulate

Es existiert derzeit kein Protection Profile für Chipkartenleser zum Einsatz im Rahmen SigG/SigV.

9. Literaturverzeichnis

	Referenz	Beschreibung
[1]	CT-API	Deutsche Telekom AG (PZ Telesec), GMD Darmstadt, TÜV Informationstechnik GmbH, TeleTrusT Deutschland e.V. *Anwendungsunabhängiges CardTerminal Application Programming Interface (CT-API) für Chipkartenanwendungen*, Revision 1.1, 14. 10. 1998. Publiziert in MKT Spezifikation [2, Teil 3].
[2]	CT-BCS	TeleTrusT Deutschland e.V. *Multifunktionale KartenTerminals (MKT) – Spezifikation, Teil 4: Anwendungsunabhängiger CardTerminal Basic Command Set (CT-BCS)*, Version 1.0, 15. 04. 1999.
[3]	PC/SC	PC/SC Workgroup *Interoperability Specification for ICCs and Personal Computer Systems, Revision 1.0, December 1997* http://www.pcscworkgroup.com *Anmerkung: die vorliegende Spezifikation V2.0 wird nicht unterstützt, da diese weltweit noch nicht relevant ist.*
[4]	ISO/IEC 7816	International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC) *Information technology -- Identification cards -- Integrated circuit(s) cards with contacts -- Part 4: Interindustry commands for interchange*, 2005-01-05 und *Information technology -- Identification cards -- Integrated circuit(s) cards with contacts -- Part 8: Commands for security operations*, 2004-06-11
[5]	Class 2	Informatikzentrum der Sparkassenorganisation GmbH *Definition Anforderungen an Chipkartenleser für den Heimbereich aus Sicht der SKO, Version 1.0 (09/97)* (Unveröffentlichtes Manuskript)
[6]	Signaturgesetz	*Gesetz über die Rahmenbedingungen für elektronische Signaturen und zur Änderung weiterer Vorschriften (Signaturgesetz – SigG) vom 16. 05. 2001* BGBl. I, S. 876ff, 21. 05. 2001. Geändert durch Erstes Gesetz zur Änderung des Signaturgesetzes (1. SigÄndG) vom 04. 01. 2005, BGBl. I, S. 2f, 10. 01. 2005.
[7]	Signaturverordnung	*Verordnung zur elektronischen Signatur (Signaturverordnung – SigV) vom 16. 11. 2001* BGBl. I, S. 3074ff, 21. 11. 2001. Geändert durch Erstes Gesetz zur Änderung des Signaturgesetzes (1. SigÄndG) vom 04. 01. 2005, BGBl. I, S. 2f, 10. 01. 2005.
[8]	CCID	USB Implementors Forum, Inc.; Device Working Group (DWG). Universal Serial Bus Device Class Specification for USB Chip/Smart Card Interface Devices, Revision 1.00, March 20, 2001. http://www.usb.org *Anmerkung: die neuere Version 1.1 unterscheidet sich nur marginal von Version 1.0 bei Fehlercodes. Um die Rückwärts-Kompatibilität zu erhalten, arbeiten wir mit Version 1.0*

[9]	BSI Siegel	Bundesamt für Sicherheit in der Informationstechnik (BSI). *Druckschrift7500: Produkte für die materielle Sicherheit* Oktober 2000.
[10]	EMV 2000	EMVCo LLC. *EMV™ Integrated Circuit Card Specifications for Payment Systems* Version 4.0, 2000. http://www.emvco.org *Anmerkung: die neue Version 4.1 wird weltweit noch nicht genutzt. Daher verwenden wir Version 4.0*
[11]	Common Criteria	*Common Criteria – Gemeinsame Kriterien für die Prüfung und Bewertung der Sicherheit von Informationstechnik* Version 2.1, August 1999. Deutsche Übersetzung des englischen Originals.
[12]	SigG-Alg	Bundesnetzagentur (vormals: Regulierungsbehörde für Telekommunikation und Post) *Bekanntmachung zur elektronischen Signatur nach dem Signaturgesetz und der Signaturverordnung (Übersicht über geeignete Algorithmen) vom 02. 01. 2005*, Bundesanzeiger Nr. 59, S. 4695f, 30. 03. 2005.
[13]	OCF	OpenCard Consortium *OpenCard Framework V1.2 API Documentation* Fourth Edition, December 1999 http://www.opencard.org
[14]	ANSI X9.62	American National Standard Institute ANSI X9.62. Public Key Cryptography: The Elliptic Curve Digital Signature Algorithm (ECDSA), 1998. http://www.ansi.org bzw. http://www.x9.org
[15]	IEEE 1363	Institute of Electrical and Electronics Engineers, Inc. *IEEE 1363 Standard specifications for public key cryptography.* 2000 http://grouper.ieee.org/groups/1363/P1363
[16]	FIPS 180-2	[American] National Institute of Science and Technology (NIST) *Secure Hash Standard, Federal Information Processing Standard (FIPS) 180-2*, August 2002.
[17]	FIPS 186-2	[American] National Institute of Science and Technology (NIST) *Digital Signature Standard, Federal Information Processing Standard (FIPS) 186-2*, Januar 2000.
[18]	ISO/IEC 15946-2	International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC) *Information technology -- Security techniques -- Cryptographic techniques based on elliptic curves -- Part 2: Digital signatures* 2002-11-25
[19]	ISO/IEC 10118-3	International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC) *Information technology -- Security techniques -- Hash-functions -- Part 3: Dedicated hash-functions* 2004-02-24
[20]	B0/B1	PZ Telesec der Deutschen Telekom AG, Netphen *HTSI Programmierhandbuch, Programmierhandbuch zum Host Transport Service Interface* Version 1.0

10. Abkürzungsverzeichnis

CC	Common Criteria
CCID	Integrated Circuit(s) Cards Interface Device
CT	Card Terminal
CT-API	Card Terminal Application Programming Interface
ECDSA	Elliptic Curve Digital Signature Algorithm
EMV	Europay / Mastercard / VISA
EVG	Evaluationsgegenstand
HBCI	Home Banking Computer Interface
I2C	Inter IC Bus
OCF	Open Card Framework
PC/SC	Personal Computer / Smart Card Interface
PIN	Personal Identification Number
SHA-1	Secure Hash Algorithm 1
SigG	Signaturgesetz
SigV	Signaturverordnung
SSEE	Sichere Signaturerstellungseinheit
VPN	Virtual Private Network
WHQL	Windows Hardware Quality Labs